What will we learn from the Market Failure of Digital Identity?

Stephen Wilson, Lockstep Consulting

with George Peabody, Glenbrook Partners

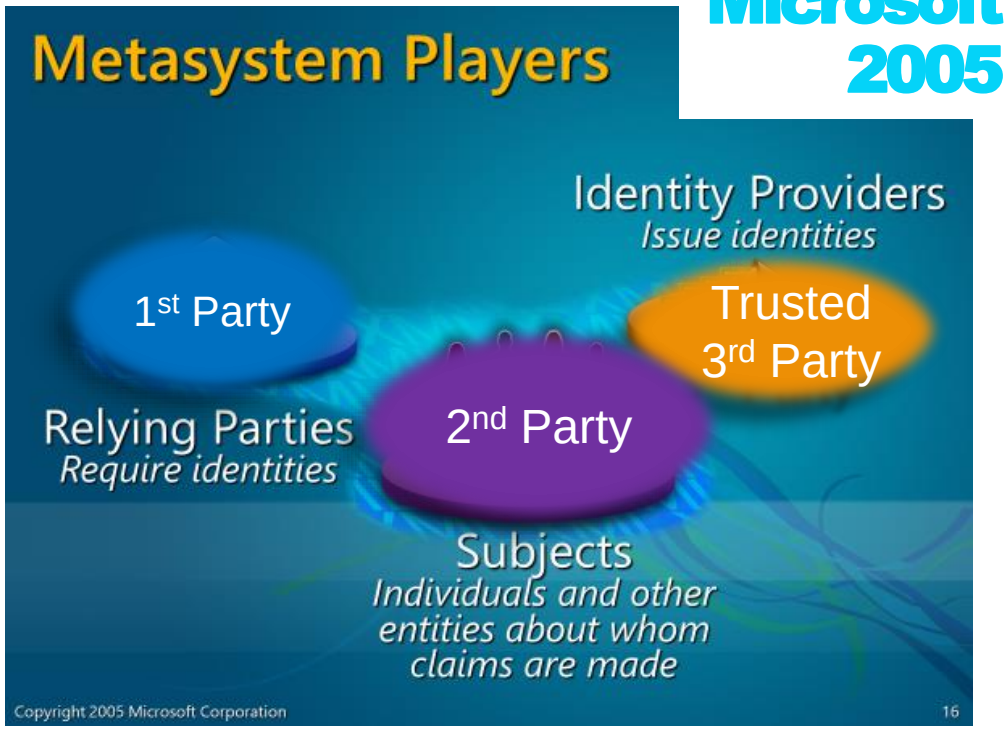
Identiverse 2022, June 23, Denver.

A paradigm is a suite of “universally recognized achievements that for a time provide model problems and solutions for a community of practitioners”. We have all been working in a *digital identity paradigm* ever since the late great Kim Cameron published the Laws of Identity in 2005. Our industry’s achievements are many, including robust standards, cryptographically Verifiable Credentials, and a body of knowledge and professional practices. We have a widely accepted Standard Model or architecture, in which Subjects, Identity Providers and Relying Parties (aka Holders, Issuers and Verifiers) hold, present, exchange, use and/or consume digital identities.

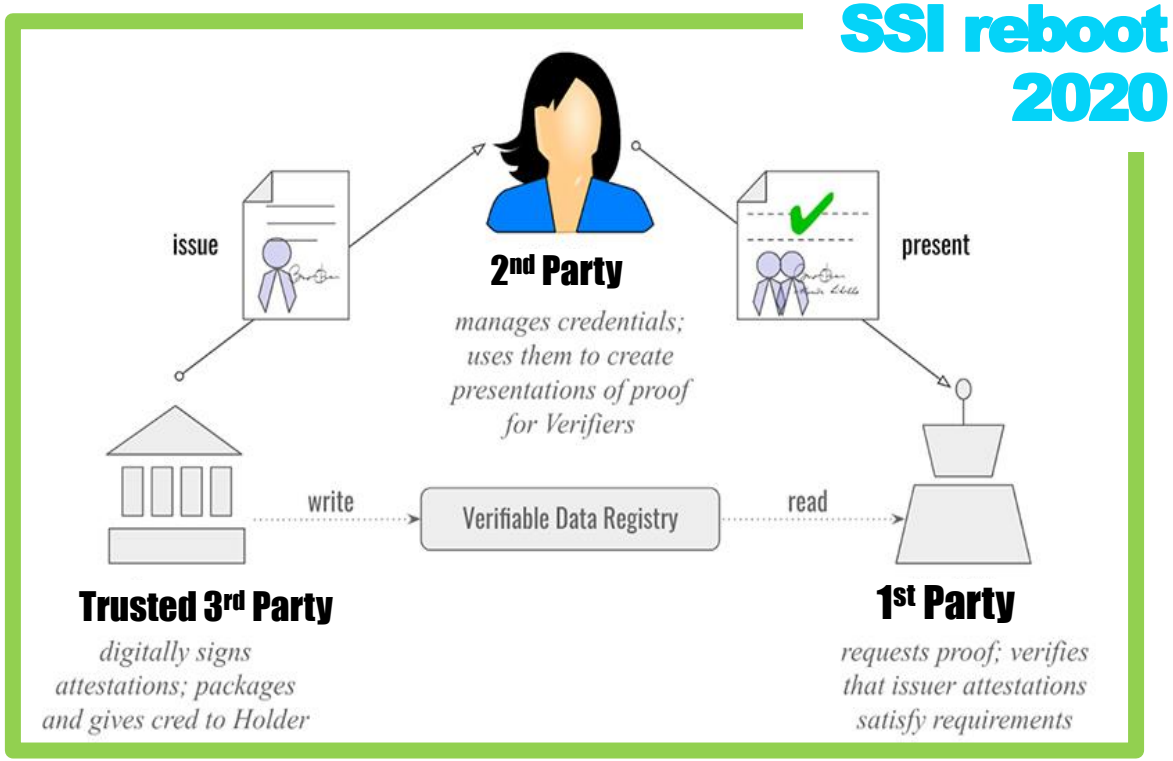
The problem is this model remains mostly hypothetical. Decades ago, the United States, Canada, Britain and Australia decided to leave it up to the free market to develop digital identity services. Yet this simply has not happened, not in any way like the ecosystem envisaged by those governments' elaborate trust frameworks and the Laws of Identity. The uncomfortable truth is that digital trust has been a market failure, but the good news is we are primed for a true paradigm shift, where the standard model is overturned, the Identity problem reframed, and our digital tools and practices repurposed.

The Standard Model of Digital Identity

Microsoft 2005



SSI reboot 2020



We have all been working in a digital identity paradigm ever since the late great Kim Cameron developed the Laws of Identity. The canonical players — *Subjects, Identity Providers* and *Relying Parties* — hold, present, exchange, use and consume digital identities as if identity is some sort of merchantable good. There has been a recent update to the terminology: now we have *Holders*, *Issuers* and *Verifiers*. But the SSI reboot has not revisited the standard model which imagines that identity can be “provided” as a good or a service.

Now, let me be clear that this presentation is about the market failure of the *standard model of identity*. Obviously digital identity is good business and at some levels is thriving, but not within the framework that was envisaged.

Grand federation: NSTIC 2011

> *Imagine if a student could get a digital credential from her cell phone provider and another from her university and use them to log in to her bank, e-mail, and social network* — Howard Schmidt.

Low level federation protocols emerged; SAML, OAUTH and OIDC quickly became widespread plumbing in day-to-day Internet logon. These prototype experiences energised the sector and led to grand visions for federated identity. The foundational proposition of NSTIC for example was set out by White House security adviser Howard Schmidt in 2011 (Ref: https://obamawhitehouse.archives.gov/blog/2011/01/07/national-program-office-enhancing-online-trust-and-privacy).

That promise was based on social logon, but it was a radical extrapolation. Social logon — i.e. federated identity at assurance level 0 — is easy because nothing much matters: the “identity provider” doesn’t know who you are and the Relying Party doesn’t care who you are.

After nearly a decade NSTIC folded. It never came got close to the vision.

We left it for the markets

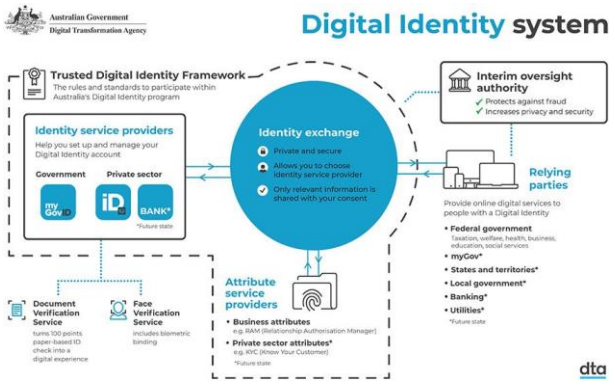
Well before NSTIC, the United States, Canada, Britain and Australia (the largest Common Law system countries) decided to leave the free market to come up with digital identity services. Yet this simply has not happened, not in any way like the ecosystem envisaged by those governments' elaborate trust frameworks and the Laws of Identity.

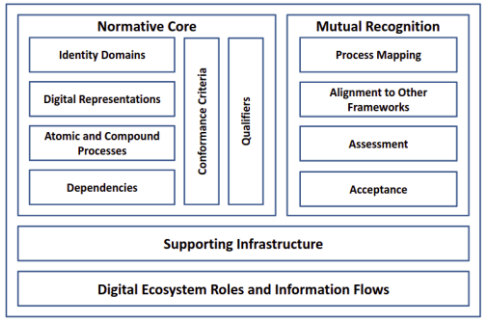
[The U.K.] looks to the establishment of a range of authentication services by central and local government and the private sector, and for public sector bodies to use these — U.K. Cabinet (2000).

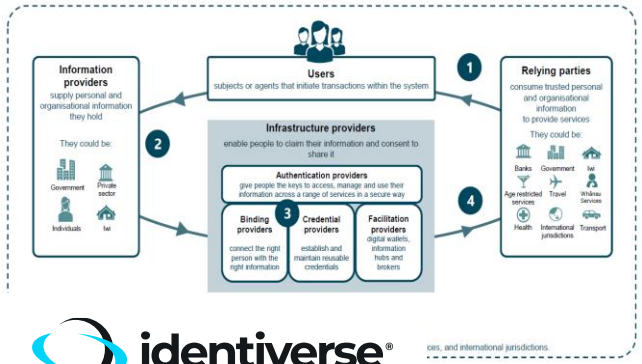
The vibrant marketplace will provide choices of identity providers, both private and public, and of multiple credentials — IDESG (2012)

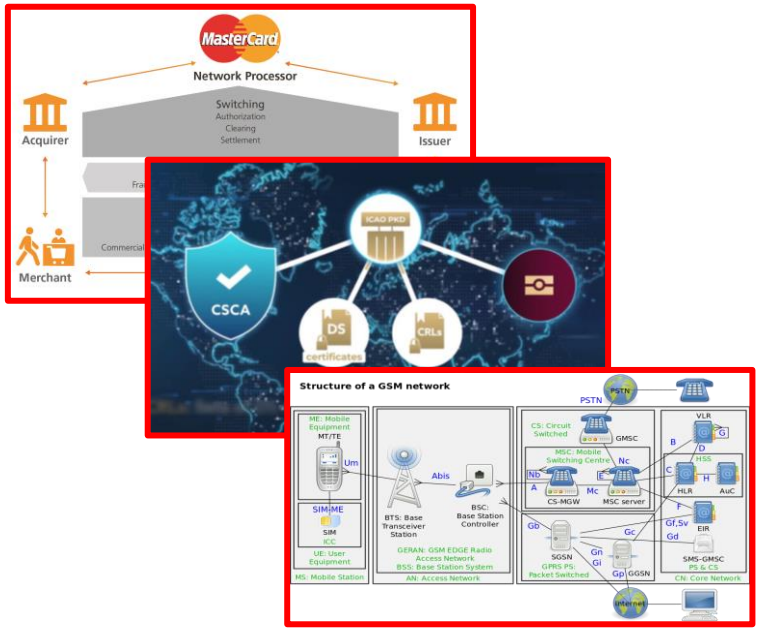
Private sector will lead the effort — NIST (2012).

Trust Frameworks: Digital Identity's Happy Place









In parallel with Digital Identity, a whole governance industry has sprung up. SSI advocate Nick Byrne has called out the movement's "over-emphasis on governance" (Ref: https://nickbyrne.substack.com/p/the-challenge-for-self-sovereign, 2020).

A happy place for identity governance is the *trust framework*. In 2010 the new Open Identity Exchange (OIX) released its first whitepaper, featuring the *Open Identity Trust Framework.* Since then, Canada, New Zealand, Australia and numerous industry groups have published trust frameworks. By 2015, there were so many that the Kantara Initiative felt the need for a survey, and found 103 of them. This month (June 2022) OIX published an overarching guide, which sets out 30 elements of "Smart Digital ID" trust frameworks.

The first thing most experts say about trust frameworks is the world has lots of trust frameworks, citing credit cards, e-passports, driver licensing, telephony networks and professional certifications. And yet we keep trying to write new ones!

What we need is better analog-to-digital conversion, in context, of the many trust frameworks we already rely on.

A paradigm shift. Really.

Paradigm: “Universally recognized scientific achievements that, for a time, provide model problems and solutions for a community of practitioners”

— Thomas Kuhn, 1962.

Paradigm is an overused buzzword but it really is apt in our case. Remember the technical meaning of paradigm, given by the philosopher of science, Thomas Kuhn. The digital identity industry has many achievements for sure, which we will recount later in this presentation. The key thing about a paradigm is how it sets a way of looking at the world; in casual usage, we tend to forget Kuhn’s emphasis on *model problems* and *model solutions*.

Our industry has focused on solving for *the re-use of digital identity*. We have rarely examined how the poor usability of digital identity is mostly a human factors problem. The paradigmatic digital identity technology is passwords, a technique borrowed from 1960s mainframe operators and inflicted on hundreds of millions of consumers on the Internet. The password must be the only technology which is *difficult to use by design*; its efficacy *depends* on it being difficult to remember. Far superior consumer access technologies preceded passwords; just think of house keys and car keys (things that we would never dream of federating).

I believe the identity industry is probably in a paradigm shift right now. It’s a big call; usually only time will tell. So how can we pick a paradigm shift as it’s happening? There are clues all around us.

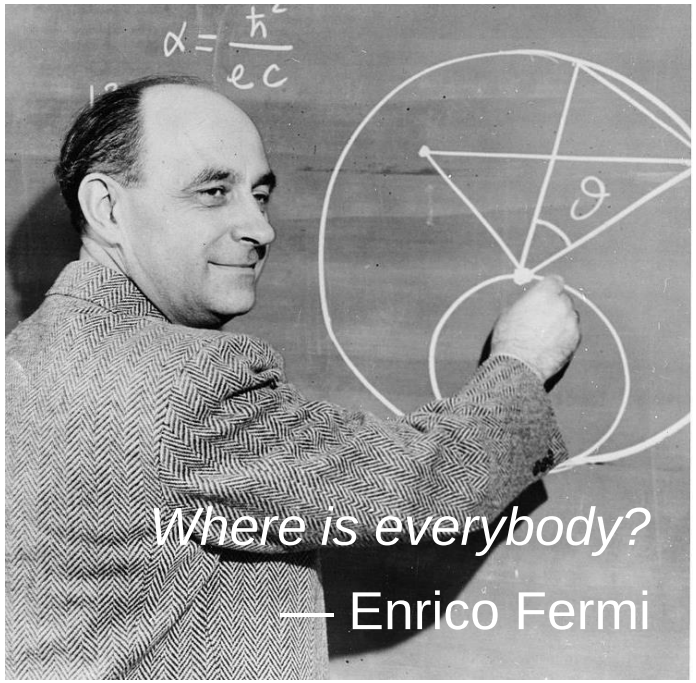
Identity industry paradoxes

Strong clues that a scientific paradigm is breaking down come from paradoxes: observations that just don't make sense. The signs of an identity shift are all around us.

For one thing, there's a sort of "Fermi Paradox" in our industry (recall the great physicist's argument that if life is inevitable in the universe, then we should see aliens since there has been so much time for them to spread across the cosmos). If digital identity is such a good idea and such an urgent requirement, then the world should have plenty of IdPs by now.

What's more, the most important developments in our industry are not in fact about identity!

The FIDO Alliance — by far the most impactful identity industry group — was never about identity. Verifiable Credentials shift the focus from *who you are* to *what you are*; we can now load a driver licence or vaccination certificate onto a smart watch, yet these are not identification tokens. And Phil Windley, one of SSI's godfathers, has said repeatedly "there's no artifact called an 'identity' in self sovereign identity". SSI instead is about relationships and credentials.



fido ALLIANCE

identiverse

#identiverse

Digital Identity is not what we thought it was

It turns out that digital identity is not what we thought it was. Our intuitions were false, just like pre-Copernican concepts of the solar system. Identity is not a good or a service. Windley is correct: what we badge “digital identity” is really about relationships and credentials.

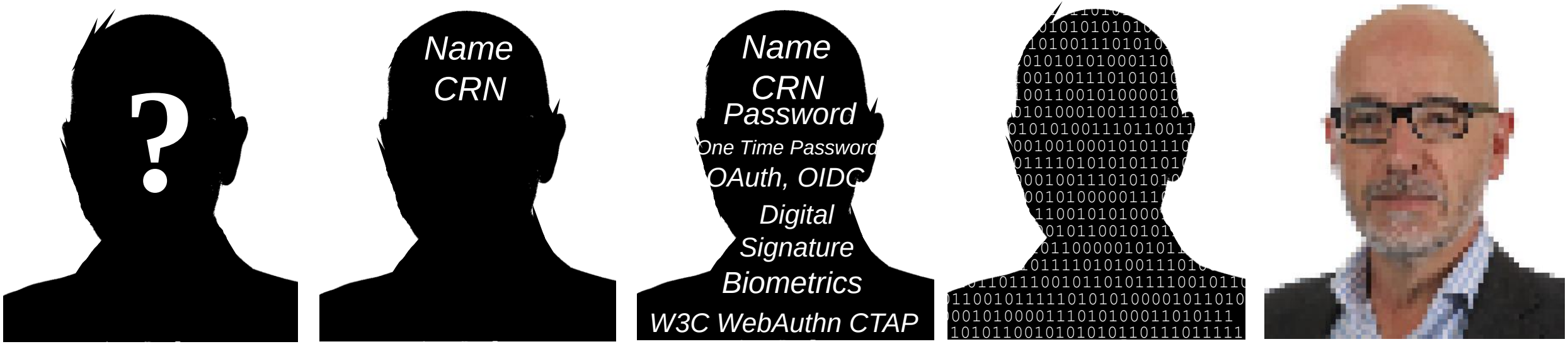
So let’s do a reality check.

We know that relationships don’t easily “federate”. Alice can have a great relationship with Bob, and Bob can have a great relationship with Carol, but none of that predicts how Alice and Carol will get along.

Now think about credentials. Usually they are highly specific. For example, no matter how good my accountant might be, I don’t want her to do my root canal. And credentials are contextualised; each country has its own professional bodies and professional standards, so overseas trained doctors don’t get to practice automatically in another country.

If digital identity is really about credentials and relationships, that explains why the Standard Model has failed.

So what is digital identity?



How do you know me? Do you know me by my name and/or a customer reference number? Those things are data.

Do you know me through additional factors, such as *what I know* and *what I have*? How do you know these factors belong to me or are under my control? For that we need binding, such as signatures and challenge-response protocols. These additional layers create metadata for confidence in the core facts & figures. And metadata is just more data.

Our multimedia world and the looming metaverse make this reality all the more vivid: Data is all we got!

And let's be really careful about this. *Digital* identity can't be anything else than data.

I've been socialising this view now for about three years and I get a lot of push-back. Some accuse me of being reductionist. But honestly I am looking for common ground: building blocks and design patterns that we can all agree on.

Reframe: Design Thinking for the RP

Now, if “It’s The Data, Stupid”, then the model questions in the digital identity paradigm may be wrong. So let’s reframe. Let’s try some design thinking, from the perspective of the Relying Party. When designing a new transaction system, we should ask: What do you need to know? Where will you get that information? And how will you satisfy yourself that it is true? Note that the lines of inquiry triggered by those sorts of questions overlap with many of the hottest topics in cyber security and policy today: sources of truth, authorship, provenance and authenticity.

I wonder can we agree that counterparties need to know things about each other? Can we agree that online, the primitive actions are about data and signals about data quality?

“Identity”, credentials, Assertions, Attributes, Claims, Authenticate, Authorize, KYC …

Sources of truth, Issuers, registries, Certification Authorities, DID Documents, X.509 …

Authorship, attestation, notarisation, Digital Signatures, proof of possession, device metadata …

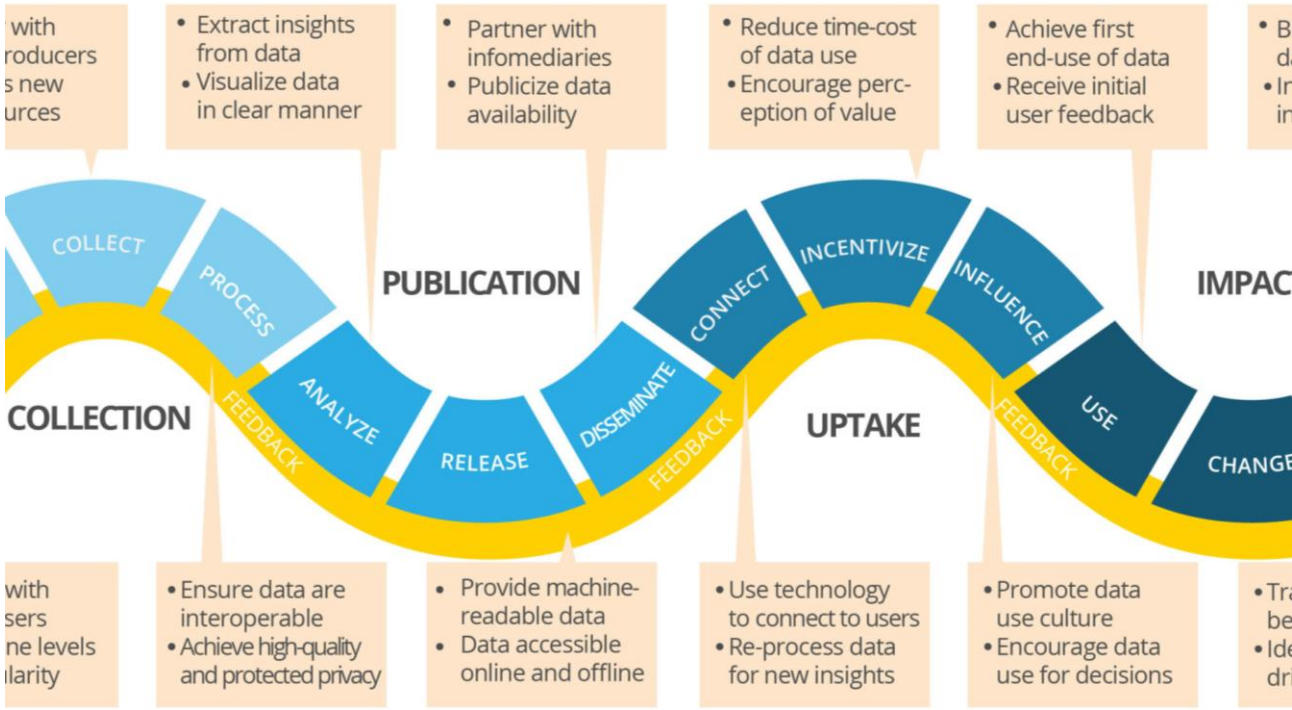
We have the tools for a higher purpose

So that's how I see our industry's successes: superb tools for delivering quality signals about data. We have achieved much.

- The FIDO Alliance is the best standardisation effort so far.
- Verifiable Credentials are a classic design pattern (with us for 30 years in SIMs and chip cards) in which a fact about the holder is wrapped in a signed object to prove where the fact came from. VCs are an ensemble of *data* and *metadata* about origin, proof of possession, policy qualifiers, cryptographic key management etc.
- Cryptographic wallets are a potent combination of cryptographic processing, secure storage, access control and compact certifiable code. Wallet capability is being automated and integrated into IoT devices for automatic verification of warranty, service history, authenticity of components and so on.

The common law system countries (AU, CA, NZ, UK & US) left the market to work out identity, and the market "decided" that there's no need for IdPs. Let us respect that decision. The market has been trying to tell us for over a decade: IDENTITY IS NOT FOR SALE!

At the same time, data value chains have developed throughout society. We know that data is big business, for good and for bad. We need the data market to be more orderly, more transparent, more accountable, more purposeful. The work of the digital identity industry can be applied to this bigger and more urgent problem: the reliability and accountability of all data in the digital economy.



Credit: The Data Value Chain, Open Data Watch (detail, 2018). Attribution 4.0 International (CC BY 4.0)